Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended)
Claim 2 (currently amended)
Claim 3 (currently amended)
Claim 4 (cancelled)
Claim 5 (cancelled)
Claim 6 (currently amended)
Claim 7 (currently amended)
Claim 8 (currently amended)
Claim 9 (cancelled)
Claim 10 (cancelled)
Claim 11 (cancelled)
Claim 12 (currently amended)
Claim 13 (currently amended)
Claim 14 (cancelled)
Claim 15 (currently amended)
Claim 16 (cancelled)
Claim 17 (cancelled)
claim 18 (cancelled)
Claim 19 (currently amended)

Claim 20 (previously amended)

Claim 21 (currently amended)

Claim 22 (currently amended)

Claim 23 (previously amended)

Claim 24 (currently amended)

Claim 25 (previously amended)

Claim 26 (new)

Claim 27 (new)

Claim 28 (new)

Claim 29 (new)

Claim 30 (new)

Claim 31 (new)

1. (Currently amended)

A method of creating certificates with redundant information to certify several keys, wherein each of the certificates comprises a defined number of data elements which at least contain information on a certification body or [[( ]] issuer of the certificate[[ )]], a user of the certificate and a key certified by the certificate,comprising the following steps:

a) creation by the certification body of a basic certificate for use in connection with the several keys of the user, the basic certificate containing a single ~~recitaiton~~ recitation of a defined number of data elements therein which elements are identical or redundant if repeated in separate certificates one for each of the several keys of the user in conjunction with the certification body;

b) addition of an identifying characteristic to the basic certificate;

c) generation of a digital signature for the basic certificate;

d) addition of the digital signature to the basic certificate;

e) generation of a key pair;

f) creation of a supplementary certificate for the basic certificate which does not recite the redundant data elements contained in the basic certificate but does contain a key as set out in step e), the identifying

characteristic as set out in step b) and additional data fields not registered by the basic certificate;

g) generation of a digital signature for the supplementary certificate;

h) addition of the digital signature to the supplementary certificate; and

i) use of the basic certificate created in step a) for other of the several keys in additional supplementary certificates that share with the supplementary certificate of step f) the redundant information recited the basic certificate but like the supplementary certificate of step f) do not recite the redundant data elements.

2. (Currently amended)

The method in accordance with Claim 1, characterized in that the basic certificate does not contain any keys but comprises the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user, and
- an identifying characteristic of the basic certificate.

3. (Currently amended)

The method in accordance with Claim 2, characterized in that the supplementary certificates do not contain the redundant information recited in the basic certificate but comprise the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- a validity period of the certificate,
- extensions, and
- [[an]] the identifying characteristic of the basic certificate.

4. (Cancelled)

5. (Cancelled)

6. (Currently amended)

The method in accordance with Claim 1 where one key is to be certified in step i) and the basic certificate of step a) already exists, including the following steps:

aa) definition of the basic certificate and reading of the identifying characteristics of the basic certificate ;

bb) generation of a new key pair ;

cc) creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys of step bb) is inserted into the supplementary certificate ~~in step bb)~~ ;

dd) insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate ;

ee) generation of a digital signature for the supplementary certificate; and

ff) addition of the digital signature to the supplementary certificate.

7. (Currently amended)

The method in accordance with Claim 6, characterized in that any supplementary certificates each contain the following data elements:

- a signature algorithm,
- a key,
- a serial number of the key,
- validity period of the certificate,
- extensions, and
- the identifying characteristic of the basic certificate.

8. (Currently amended)

The method for creating a certificate for simultaneous certification of several keys with the same validity period, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body [[( ]] or issuer of the certificate[[ )]], the user of the certificate and the [[key]] keys certified by the certificate, ~~characterized by~~ comprising the following steps:

aa) generation of several key pairs;

bb) generation of a single joint or group certificate ~~(group certificate)~~ for several keys with all data elements necessary for the individual keys and keys generated in step aa), with the group certificate containing only a single recitation of data elements applicable to all keys, wherein the group certificate contains the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,
- type or version of the group certificate,
- number and types of keys,
- the several keys,
- validity,
- a serial number, and
- any extensions;

cc) generation of a digital signature for the group certificate; and

dd) addition of the digital signature to the group certificate.

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Currently amended)

The method in accordance with Claim 8, characterized in that the [[key]] keys [[is a]] are public [[key]] keys.

13. (Currently amended)

The method in accordance with Claim 1, characterized in that the basic certificate and the supplementary ~~certificate~~ certificates are stored in a non-volatile memory of a chipcard.

14. (Cancelled)

15. (Currently amended)

The method of claim 13 for determining if [[a]] the chipcard contains a relevant key to sign a message in the chip cards nonvolatile storage medium comprising:

a) check of the nonvolatile storage medium for presence of basic certificates;

b) if a basic certificate is present, identification of a supplementary certificate with a suitable signature key ;

c) reading-in of the supplementary certificate into the ~~chapcard~~ chipcard RAM;

d) definition of the identification number of the basic certificate from the supplementary certificate; and

e) reading-in of the basic certificate into the RAM.

~~f) when no basic certificate is identified checking of the storage medium for presence of group certificates; and~~

~~g) reading-in of a necessary group certificate into the RAM.~~

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Currently amended)

A computer program product on a computer usable medium for creating certificates to certify several keys sharing redundant information, wherein a certificate comprises a defined number of data elements which at least contain information on the certification body [[( ]] or issuer to the certificate[[ )]], the user of the certificate and the key certified by the certificate, said computer program product comprising:

a) software code for specification of a request for certification of one of the several keys by a certification body for a user;

b) software code for creation of a basic certificate that does not contain any key for the user ~~with~~ but does contain a defined number of data elements which, in the certification process, are identical or redundant for the several keys of respective user in conjunction with the respective certification body when initially ~~only~~ not more than one of the several keys is to be certified~~, and no~~ with the basic certificate ~~is yet available for the user~~;

c) software code for the addition of an identifying characteristic to the basic certificate;

d) software code for the generation of a digital signature for the basic certificate;

e) software code for the addition of the digital signature to the basic certificate;

f) software code for generation of a key pair;

g) software code for creation of a supplementary certificate for the basic certificate with a key pair generated with the software as set out in f), the identifying characteristic as set out in c) and additional data ~~fields~~ elements not registered by the basic certificate of b);

h) software code for generation of a digital signature for the supplementary certificate;

i) software code for addition of the digital signature to the supplementary certificate; and

j) software code for use of the basic certificate created in step b) with a future key that shares the redundant ~~information~~ data elements with the basic certificate by issuing an additional supplementary certificate with a new key pair generated with software as set forth in f), the identifying certificate as set forth in c) and additional data elements not registered by the basic certificate of b) or the supplementary certificate of g).

20. (Previously amended)

The computer program product in accordance with Claim 19, characterized in that the basic certificate comprises the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,and
- identifying characteristic of the basic certificate.

21. (Currently amended)

The computer program product in accordance with Claim 19, characterized in that the supplementary certificates comprise the following data elements:

- a signature algorithm,
- a public key from the key pair of f) or a public key from the new key pair of j),
- a serial number of the key,
- a validity period of the certificate,
- extensions, and
- identifying characteristic of the basic certificate.

22. (Currently amended)

The computer program product in accordance with Claim 19, more than one key with the same validity period is to be certified at one time, including the following software code:

aa) software code for generation of several key pairs;

bb) software code for generation of ~~the basic certificate of step b) as~~ a single group certificate ~~(group certificate)~~ for ~~several keys~~ the more than one key with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements for the several keys by having only a single recitation of the redundent data elements in the group certificate;

cc) software code for generation of a digital signature for the certificate; and

dd) software code for addition of the digital signature to the certificate.

23. (Currently amended)

The computer program product software in accordance with Claim 22, characterized in that the group certificate contains the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,
- type [[/]] or version of the certificate,
- number and types of keys,
- a key,
- validity,

- serial Number, and
- extensions.

24. (Previously amended)

The computer program product in accordance with Claim 19, where a key is to be certified and the basic certificate already exists, including the following software code:

aa) software code definition of the basic certificate and reading of the identifying characteristics of the basic certificate;

bb) software code for generation of a key pair;

cc) software code for creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate by step bb);

dd) software code for insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate;

ee) software code for generation of a digital signature for the supplementary certificate; and

ff) software code for addition of the digital signature to the supplementary certificate.

25. (Previously amended)

The computer program product in accordance with Claim 24, characterized in that the supplementary certificate contains the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- validity period of the supplementary certificate,
- extensions, and
- identifying characteristic of the basic certificate.

26. (New)

A method of creating and using certificates to certify several keys for use in connection with a chipcard, wherein each of the certificates comprises a defined number of data elements which at least contain information on a certification body or issuer of the certificate, a user of the certificate and a key certified by the certificate,comprising the following steps:

a) creation by the certification body of a basic certificate that does not contain a key but is for use in connection with the several keys of the user, the basic certificate containing a single recitation of a defined number of data elements therein which elements would be identical or redundant if contained in separate certificates one for each of the several keys of the user in conjunction with the certification body;

b) addition of an identifying characteristic to the basic certificate;

c) generation of a digital signature for the basic certificate;

d) addition of the digital signature to the basic certificate;

e) generation of a key pair;

f) creation of a supplementary certificate for the basic certificate which does not recite the redundant data elements contained in the basic certificate but does contain a key as set out in step e), the identifying characteristic as set out in step b) and additional data fields not registered by the basic certificate;

g) generation of a digital signature for the supplementary certificate;

h) addition of the digital signature to the supplementary certificate;

i) use of the basic certificate created in step a) for other of the several keys in additional supplementary certificates that share with the supplementary certificate of step f) the redundant information recited the basic certificate but like the supplementary certificate of step f) do not recite the redundant data elements; and

j) storage of the basic and supplementary in a nonvolatile memory of the chipcard.

27. (New)

The method in accordance with Claim 26, characterized in that the basic certificate comprises the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user, and
- an identifying characteristic of the basic certificate.

28. (New)

The method in accordance with Claim 26, characterized in that the supplementary certificates comprise the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- a validity period of the certificate,
- extensions, and
- the identifying characteristic of the basic certificate.

29. (New)

The method in accordance with Claim 26, where more than one key with the same validity period are to be certified at one time in step f), including the following steps:

aa) generation of several key pairs one for each of the keys;

bb) generation of a single certificate for all the several keys with all data elements necessary for the individual keys and keys generated in step aa), with only a single recitation of data elements redundant to all the several keys in the gro9up certificate;

cc) generation of a digital signature for the group certificate;

dd) addition of the digital signature to the group certificate; and

ee) group certificate in the nonvolatile memory of the chipcard.

30. (New)

The method in accordance with Claim 27, characterized in that the basic certificate contains the following data elements:

- name of the certificate body,
- user ID of the certification body,
- name of the user,
- user ID of the user,
- type or version of the certificate,
- number and types of keys,
- a key,
- validity,
- serial number, and
- extensions.

31. (New)

The method of Claim 29 for determining if the chipcard contains a relevant key in the chipcards nonvolatile storage medium to sign a message:

a) check of the nonvolatile storage medium for presence of basic certificates;

b) if a basic certificate is present, identification of a supplementary certificate with a suitable signature key;

c) reading-in of the supplementary certificate into the chipcard RAM;

d) definition of the identification number of the basic certificate from the supplementary certificate;

e) reading-in of the basic certificate into the RAM;

f) when no basic certificate is identified checking of the storage medium for presence of group certificate; and

g) reading-in of a necessary group certificate into the RAM.